Une méthode de Newton pour la décomposition de Dunford

Proposition 0.1. *Soit $\mathbb{K}$ un corps de caractéristique nulle et A une matrice de $\mathcal{M}_n(\mathbb{K})$, de polynôme caractéristique χ_A et de décomposition de Dunford $A = D + N$. On pose $P := \frac{\chi_A}{\chi_A \wedge \chi_A'}$ et on considère la suite de matrices (A_r) donnée par*

$$A_0 = A,\ A_{r+1} = A_r - P(A_r)P'(A_r)^{-1}.$$

Alors, cette suite est bien définie, elle est stationnaire et tend vers D. Plus précisément $A_m = D$ pour tout $m \geq \log_2(n)$.

Démonstration. Tout d'abord, le fait que $\mathbb{K}$ est de caractéristique nulle fait que χ_A' ne s'annule pas et donc, que P est bien défini. C'est bien un polynôme puisque le PGCD $\chi_A \wedge \chi_A'$ divise χ_A, et de plus, ses racines λ_i sont aussi racines de χ_A. Soit $m_i \geq 1$ la multiplicité de λ_i dans χ_A, de sorte que $\chi_A = (X - \lambda_i)^{m_i} Q$, où Q est un polynôme qui ne s'annule pas en λ_i. Alors $\chi_A' = m_i(X-\lambda_i)^{m_i - 1}Q + (X - \lambda_i)^{m_i}Q'$, et comme, en caractéristique zéro, le premier terme est non nul, il vient que λ_i est racine de χ_A' avec multiplicité $m_i - 1$. Conclusion, P a pour racine les λ_i et ce sont des racines simples.

Nous allons maintenant montrer par récurrence sur $r \geq 0$ que :

(i) la matrice $P(A_r)$ est nilpotente d'indice de nilpotence $\nu_r \leq 1 + \frac{n-1}{2^r}$,

(ii) la matrice $P'(A_r)$ est inversible,

(iii) la matrice A_{r+1} est bien définie et appartient à $\mathbb{K}[A]$.

Montrons que cela prouve la proposition. Effectivement, si on suppose vrai ces trois assertions, alors (A_r) est bien définie, et les A_r commutent entre eux. On a de plus que $P(A_m)$ est d'indice de nilpotence $\nu_m = 1$ pour $m \geq \log_2(n)$; $P(A_m)$ est donc nulle et la suite est bien stationnaire. Comme P est à racines simples, A_m est diagonalisable. De plus,

$$\begin{aligned} A - A_m &= (A_0 - A_1) + (A_1 - A_2) + \cdots + (A_{m-1} - A_m) \\ &= P(A_0)P'(A_0)^{-1} + P(A_1)P'(A_1)^{-1} + \cdots P(A_{m-1})P'(A_{m-1})^{-1}. \end{aligned}$$

Or, $P(A_r)P'(A_r)^{-1}$ est nilpotente, puisque $P(A_r)$ l'est et que $P(A_r)$ et $P'(A_r)^{-1}$ commutent (comme A_r est dans $\mathbb{K}[A]$). On a donc que $A - A_m$ est nilpotente puisque c'est une somme de matrices nilpotentes, qui, de plus, commutent deux à deux (ce sont des polynômes en A). On conclut que $A - A_m$ est nilpotent et commute à A_m qui est diagonalisable. Par unicité de la décomposition de Dunford, $A_m = D$.

Reste à montrer les trois assertions, par récurrence.

Initialisation : $P(A_0) = P(A)$ est bien nilpotente puisque, comme toutes les racines de P sont racines de χ_A, on a que χ_A, qui est de degré n, divise P^n, et donc, par Cayley-Hamilton, $0_n = P^n(A) = P(A)^n$. On a donc bien que $P(A)$ est nilpotente, d'indice $\nu_0 \leq n = 1 + \frac{n-1}{2^0}$. Donc, (i) est vraie pour $r = 0$. De plus, pour montrer (ii), on peut remarquer que $P'(A)$ est inversible puisque les valeurs propres $P'(\lambda_i)$ de $P'(A)$ sont non nulle. La dernière assertion est claire, par (ii).

Hérédité : On suppose les trois assertions vraies pour r, et on veut les montrer pour $r+1$. Notons tout d'abord, que par la formule de Taylor polynomiale à l'ordre 2, il existe, un polynôme $Q \in \mathbb{K}[X,Y]$ tel que $P(a+h) = P(a) + hP'(a) + h^2 Q(a,h)$, pour tout a, h dans $\mathbb{K}$. Soit R et S deux polynômes de $\mathbb{K}[X]$, alors, pour tout x dans $\mathbb{K}$, on a $P(R(x)+S(x)) = P(R(x))+S(x)P'(R(x))+S(x)^2\tilde{Q}(x)$, pour un $\tilde{Q}$ de $\mathbb{K}[X]$. Comme $\mathbb{K}$ est de caractéristique nulle, il est infini, et cette identité reponte en une identité polynomiale dans $\mathbb{K}[X]$:

$$P(R(X) + S(X)) = P(R(X)) + S(X)P'(R(X)) + S(X)^2\tilde{Q}(X).$$

On peut alors évaluer cette identité en la matrice A, avec R tel que $A_r = R(A)$, et $S = -PT$, où T est un polynôme tel que $T(A) = P'(A_r)^{-1}$. Effectivement, par hypothèse de récurrence, $P'(A_r)$ est inversible et appartient à $\mathbb{K}[A]$, donc, par un résultat classique (qui utilise Cayley-Hamilton), l'inverse de $P'(A_r)$ est un polynôme en $P'(A_r)$, et donc un polynôme en A.

L'évaluation en A_r donne donc :

$$\begin{aligned} P(A_r - P(A_r)P'(A_r)^{-1}) &= P(A_r) - P(A_r)P'(A_r)^{-1}P(A_r) + P(A_r)^2T(A_r)^2\tilde{Q}(A) \\ &= P(A_r)^2T(A_r)^2\tilde{Q}(A). \end{aligned}$$

On en déduit $P(A_{r+1}) = P(A_r)^2T(A_r)^2\tilde{Q}(A)$. Et comme toutes les matrices commutent, $P(A_{r+1})$ est nilpotente d'indice de nilpotence vérifiant $\nu_{r+1} \leq \frac{\nu_r+1}{2}$. On montre alors facilement l'assertion (i) par récurrence sur r.

Montrons (ii). Comme le polynôme P est à racines simples, il est premier avec P' et on obtient donc une relation de Bezout : $UP + VP' = 1$. Encore une fois, l'évaluation en A_r donne $V(A_r)P'(A_r) = \mathrm{I}_n - U(A_r)P(A_r)$. Or, $U(A_r)P(A_r)$ est nilpotente par (i) (et la commutation ambiante) et donc $V(A_r)P'(A_r)$ est unipotente (son spectre est réduit à 1), et donc, de déterminant non nul. Ceci implique que $\det P'(A_r) \neq 0$, et donc (ii).

L'assertion (iii) est alors claire. Ce qui achève la preuve.

Remarque 0.2. La méthode de Newton propose une solution à l'équation $f(x) = 0$ comme limite d'une suite (u_n) définie par $u_{n+1} = u_n - \frac{f(u_n)}{f'(u_n)}$. On généralise cette méthode dans le cadre des matrices de $\mathbb{K}[A]$, qui est commutative. Le petit miracle ici est que le choix de $f = P$ fait que la suite est stationnaire (Cayley-Hamilton y est pour beaucoup). On retrouve l'idée qu'en algèbre, être petit revient à être nilpotent.

Remarque 0.3. La côté très exploitable de cette proposition vient du fait que tout se programme rapidement, sans avoir besoin de factoriser χ_A. En effet, le PGCD de χ_A et χ_A' se fait avec l'algorithme d'Euclide, qui est de complexité $n(n-1)$ (en général, c'est le produit des degrés). Les évaluations de polynômes en matrices donnent des calculs de complexité en n^3, ainsi que l'inversion de $P'(A_r)$ ce qui fait qu'au final, on a un algorithme de complexité en $n^3 \log(n)$.

Remarque 0.4. Le problème est juste si χ_A possède une racine d'ordre un multiple de p, où p est la caractéristique du corps. Si c'est le cas, P existe, est à racines simples, et on continue tranquillement l'algorithme. Sinon, c'est la catastrophe. Tout ce que l'on peut dire en général (pour tout corps), c'est que P est le génerateur de l'idéal $\{Q,\ Q(A) \text{est nilpotent}\}$ de $\mathbb{K}[X]$, mais ca aide pas à le calculer concrètement.